КВАНТОВАЯ КРИПТОГРАФИЯ

Об уязвимостях квантовой криптографии на геометрически однородных когерентных состояниях

Д.А.Кронберг

*Показано, что протокол квантовой криптографии на геометрически однородных когерентных состояниях, использующий ограничение на безошибочное различение набора симметричных когерентных состояний и позволяющий противодействовать атаке с безошибочным различением состояний (USD-атака), не является стойким к ряду других атак. Приведено сравнение формулы длины ключа из работы С.Н.Молоткова (Письма в ЖЭТФ, **101**(8), 637 (2015)) и скорости генерации ключа для ряда конструктивных атак перехватчика и показано, что скорость генерации ключа в этой работе существенно завышена. Это ведет к тому, что распределяемый ключ не является секретным.*

Ключевые слова: *квантовая криптография, когерентные состояния, квантовая теория информации.*

1. Введение

Целью квантовой криптографии [1–3], или, более точно, квантового распределения ключей, является распределение между двумя удаленными пользователями общего ключа, секретность которого не основывается на каких-либо предположениях об ограниченных возможностях перехватчика. Таким образом, распределенный ключ должен сохранять стойкость против *любых* действий (атак) перехватчика, не противоречащих законам квантовой механики. Для ряда протоколов квантового распределения ключей были получены доказательства стойкости [4–7], однако для некоторых протоколов построение доказательства стойкости против всех возможных атак является нерешенной и весьма сложной задачей.

Ряд атак в квантовой криптографии получили наибольшую известность, поскольку ярче всего демонстрируют возможности перехватчика при тех или иных технологических ограничениях у легитимных пользователей. В связи с этим при предложении нового протокола квантовой криптографии целесообразно проверить его на стойкость против наиболее известных атак. Однако из такой стойкости никак не следует, что протокол будет сохранять стойкость против всех других атак.

Протокол квантовой криптографии на геометрически однородных когерентных состояниях [8–10] нацелен на противодействие атаке с безошибочным различением состояний [11] (unambiguous state discrimination (USD-атака), встречается также название unambiguous measurement (UM-атака)). При такой атаке, возможной для линейно независимых состояний в условиях затухания, перехватчик получает из них полную информацию с некоторой вероятностью успеха. В случае неудачи перехватчик блокирует состояния, а в случае успеха отправляет их на принимающую сторону, увеличивая их интенсивность. Протокол использует конфигурацию симметричных когерентных состояний, для которых известна верхняя оценка вероятности безошибочного различения [12], что позволяет обеспечить невозможность USD-атаки на практически важных расстояниях за счет использования достаточно большого числа состояний. В работе [9] приведена формула генерации секретного ключа, которая в том числе связана с вероятностью успеха при безошибочном различении состояний.

Однако стойкость против USD-атаки еще не означает стойкости против любой другой атаки в условиях затухания. Ключевым недостатком USD-атаки с точки зрения перехватчика является то, что она не использует информацию о базисах, которую легитимные пользователи объявляют при общении по открытому каналу. В условиях использования большого числа состояний эта информация является достаточно ценной и может применяться при построении ряда других атак. В настоящей работе предлагаются атаки, которые используют данную информацию. Представлены условия, при которых рассмотренные атаки демонстрируют завышение скорости генерации ключа в [9], что ведет к несекретности распределяемых ключей.

В [12] было отмечено, что формулы для работы с симметричными когерентными состояниями не удается привести к простому виду, поэтому основные результаты работы, выраженные в графиках скорости генерации ключей и критических интенсивностей, были получены численным образом. Для каждой построенной атаки при этом будут рассмотрены физические идеи, описывающие ее принципиальную реализуемость и причины ее эффективности.

Работа организована следующим образом. В разд.2 кратко описан протокол квантовой криптографии на геометрически однородных когерентных состояниях. Разд.3 посвящен выводу формулы для скорости генерации ключа в работе [9]. В разд.4 рассмотрена наиболее концептуально простая атака в квантовой криптографии – атака светоделителем. Показано, что даже против такой атаки скорость генерации ключа является завышенной. Также описана схема подслушивания с помощью ак-

Д.А.Кронберг. Математический институт им. В.А.Стеклова РАН, Россия, 119991 Москва, ул. Губкина, 8;
e-mail: dmitry.kronberg@gmail.com

Поступила в редакцию 17 июня 2021 г.

тивного светоделителя, которая будет использоваться в дальнейших разделах. Разд.5–7 посвящены другим атакам: модифицированной атаке расщеплением по числу фотонов, атаке с усилением состояний и атаке с различением битов ключа. Для одних атак показаны скорости генерации ключа, для других – критическое значение интенсивности в зависимости от длины линии связи. В Заключении приведены основные выводы работы.

2. Протокол на геометрически однородных состояниях

Идея использования симметричных когерентных состояний в квантовой криптографии встречается в работах [13–16], а также в более поздних работах [8–10, 17, 18], причем некоторые протоколы были реализованы практически [19–21]. Приведем здесь описание протокола из работ [8–10].

Напомним, что когерентное состояние $|\alpha\rangle$ записывается как

$$|\alpha\rangle = \exp(-|\alpha|^2/2)\sum_{n=0}^{+\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle,$$

где $|n\rangle$ – базис Фока. В протоколе используются N симметричных когерентных состояний, имеющих вид [12]

$$|\alpha_j\rangle = |\alpha\exp(\mathrm{i}2\pi j/N)\rangle, \quad j = 0,\ldots,N-1,$$

т.е. у всех таких состояний интенсивности $\mu = |\alpha|^2$ совпадают, а фаза принимает значения $\{2\pi j/N\}_{j=0}^{N-1}$ из набора с равными промежутками. Поскольку N – четное число, состояния делятся на $M = N/2$ базисов. Фазовые сдвиги θ внутри каждого базиса совпадают, поэтому состояния одного базиса b, соответствующие отправке 0 и 1, имеют вид

$$\begin{aligned}|\alpha_b^0\rangle &= |\alpha\exp[\mathrm{i}2\pi k(b)/N]\rangle,\\ |\alpha_b^1\rangle &= |\alpha\exp\{\mathrm{i}[2\pi k(b)/N+\theta]\}\rangle,\end{aligned} \tag{1}$$

где исходное значение $k(b)$ для каждого базиса определяется конфигурацией состояний.

В дальнейшем будем следовать традиционным для квантовой криптографии обозначениям и будем называть легитимных пользователей Алисой и Бобом, а перехватчика – Евой.

На первом шаге Алиса случайным образом выбирает базис $b \in \{0,\ldots,M-1\}$ и бит $k \in \{0,1\}$ в каждой позиции, после чего отправляет Бобу соответствующее состояние $|\alpha_b^k\rangle$. Точнее, Алиса отправляет опорное состояние $|\alpha\rangle$, фаза которого известна и всегда одинакова [8], и информационное состояние, поэтому ее состояния имеют вид

$$|\psi_b^k\rangle = |\alpha\rangle\otimes|\alpha_b^k\rangle. \tag{2}$$

Боб получает состояние после прохождения сигналом линии связи длиной L. Когерентные состояния в оптоволоконных линиях связи преобразуются самоподобным образом, и состояние Боба в отсутствие перехватчика будет отличаться от состояния Алисы только величиной интенсивности μ, которая преобразуется в

$$\tilde{\mu} = \mu\times 10^{-\kappa L/10}, \tag{3}$$

где κ – показатель затухания в линии связи, равный для оптоволокна приблизительно 0.2 дБ/км (в дальнейшем будем использовать именно это значение).

Боб случайным образом выбирает базис и проводит безошибочное различение состояний этого базиса [22]. Теоретическая вероятность успеха при безошибочном различении состояний $\{|\tilde{\alpha}_b^0\rangle, |\tilde{\alpha}_b^1\rangle\}$, где $\tilde{\alpha} = \sqrt{\tilde{\mu}}$ (опорное состояние $|\alpha\rangle$ в (2) нужно для совершения измерения, но оно не меняет скалярных соотношений и вероятность успеха) [23] есть

$$p_{\mathrm{succ}}^{\max} = 1-|\langle\tilde{\alpha}_n^0|\tilde{\alpha}_n^1\rangle| = 1-\exp[-(1-\cos\theta)\tilde{\mu}]. \tag{4}$$

Однако на практике схема может быть менее эффективной и давать меньшую вероятность успеха. Предлагаемая в [9] схема с одним детектором и фазовым модулятором для выбора бита внутри базиса дает вероятность успеха (подробнее см. в [17])

$$p_{\mathrm{succ}} = \tfrac{1}{2}\{1-\exp[-\tfrac{1}{2}(1-\cos\theta)\tilde{\mu}]\}. \tag{5}$$

В дальнейшем для вероятности успеха при безошибочном различении состояний мы будем пользоваться именно формулой (5), хотя формула (4) и дает схожие результаты. Мы полагаем, что аппаратура легитимных пользователей работает идеально: в частности, детекторы на принимающей стороне имеют единичную эффективность и нулевой уровень темновых шумов.

После того как Алиса передает состояния во всех позициях, а Боб производит измерения, они переходят к этапу *согласования базисов*: по открытому каналу они раскрывают базисы, использованные для приготовления и измерения состояний в каждой позиции, и отбрасывают посылки в случае несовпадения (вероятность совпадения базисов составляет $1/M = 2/N$). Также отбрасываются посылки, где измерение Боба дало неопределенный исход. В результате получается *сырой ключ*.

На следующем этапе – *коррекции ошибок* – Алиса и Боб исправляют ошибки в сыром ключе, также общаясь по открытому каналу, в результате чего часть информации о ключе раскрывается. Перед этим они оценивают ошибку, раскрывая часть сырого ключа и затем отбрасывая раскрытые позиции (отметим, что существуют и более эффективные методы оценки ошибки, см., напр., [24, 25]). Утечка информации к перехватчику на этом этапе обозначается как leak, и она также учитывается при расчете длины итогового ключа. После коррекции ошибок Алиса и Боб имеют совпадающие ключи (за исключением очень малой вероятности некорректной работы модуля коррекции ошибок, которой мы будем пренебрегать в нашей работе).

На последнем этапе – *усиления секретности* – легитимные пользователи сжимают свой ключ для исключения информации перехватчика. На этом этапе важно, чтобы в формуле для длины итогового ключа использовалась корректная верхняя оценка информации противника: в этом случае его информация об итоговом ключе будет близка к нулевой. Ошибка при оценке информации противника и завышение длины ключа могут привести к тому, что часть итогового ключа окажется известной перехватчику, что неприемлемо. В разд.3 будет описана формула для длины секретного ключа из работы [9].

В работах [20, 21] упоминается о практической реализации протокола, в частности в [21] приведены наиболее

актуальные с практической точки зрения наборы параметров: интенсивность $\mu = 0.3-0.5$ фотон./имп., затухание в канале 18 дБ (что в нашей модели соответствует оптоволоконной линии связи длиной 90 км, хотя в практических системах такое затухание возможно и на других длинах линии связи), средняя наблюдаемая ошибка 3%–6%.

3. Формула для скорости генерации секретного ключа

Формула для скорости генерации секретного ключа является ключевым теоретическим элементом протокола квантовой криптографии. Фактически доказательство стойкости сводится к доказательству того факта [6, 7], что если выбирать длину окончательного ключа согласно формуле, то ключ будет секретным в соответствии с параметром секретности (подробнее про параметр секретности см. в [26]).

В качестве основной формулы для длины секретного ключа (или, что то же самое, скорости его генерации) в [9] используется формула Деветака–Винтера [27]

$$R_{\text{key}} = I(\text{A}:\text{B}) - I(\text{A}:\text{E}) = H(X|\text{E}) - \text{leak}, \qquad (6)$$

где I – взаимная информация между пользователями (A – Алиса, B – Боб, E – Ева); $H(X|\text{E})$ – условная энтропия, характеризующая нехватку информации Евы о ключе X при наличии у нее квантовых состояний, полученных при наилучшей атаке.

Из формулы (6) следует, что длина секретного ключа в пересчете на одну посылку определяется разностью между взаимной информацией легитимных пользователей и информацией перехватчика о ключе. Нетривиальной является оценка информации перехватчика: как следует из [9], она должна зависеть только от наблюдаемых на принимающей стороне параметров, а также от конфигурации состояний, которая известна легитимным пользователям. Пусть p_{click} – частота срабатывания детектора на принимающей стороне, тогда $p_{\text{loss}} = 1 - p_{\text{click}}$ – наблюдаемая вероятность потерь. К наблюдаемым параметрам относится также Q – средний уровень битовой ошибки (quantum bit error rate) в сырых ключах легитимных пользователей.

В качестве наиболее мощной атаки в условиях затухания рассматривается USD-атака. Обозначим вероятность успеха при безошибочном различении исходных состояний как p_{USD}; для этой вероятности в работе [12] дана оценка сверху. Если p_{loss} больше вероятности неудачи $1 - p_{\text{USD}}$ безошибочного различения исходных состояний, то перехватчик знает весь ключ, т.к. может провести USD-атаку. Если же уровень потерь меньше вероятности неудачи безошибочного различения, то предполагается, что оптимальная стратегия для подслушивателя – это применение безошибочного различения состояний к доле посылок δ. Фактически Ева в каждой позиции с вероятностью δ применяет безошибочное различение состояний, а в оставшейся части посылок, доля которых $1 - \delta$, проводит оптимальные индивидуальные измерения. Причем при оценке информации Евы, извлекаемой при таком измерении, предполагается, что на момент измерения Ева знает базис, однако не знает кодовую таблицу, вследствие чего ее информация оценивается через C_1 – пропускную способность за один шаг для двух векторов в одном базисе [28, 29]. Для двух чистых равновероятных состояний $\{|\alpha_b^0\rangle, |\alpha_b^1\rangle\}$

$$C_1 = 1 - h_2\left(\frac{1 - \sqrt{1 - |\langle\alpha_b^0|\alpha_b^1\rangle|^2}}{2}\right),$$

где $h_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ – бинарная энтропия Шеннона.

Также важно, что как для позиций, в которых сработало безошибочное различение, так и для позиций, в которых Ева не применяла это преобразование, она переотсылает Бобу состояния с высокой интенсивностью вместо исходных. Это делается для того, чтобы максимально компенсировать вносимые потери: в этом случае безошибочное различение можно применить к большей доле состояний.

В таком случае общая длина сырого ключа (здесь не учитывается информация перехватчика)

$$R_{\text{raw key}} = 1 - \delta + \delta p_{\text{USD}} = 1 - p_{\text{loss}},$$

из чего можно заключить, что доля посылок δ, к которым применяется безошибочное различение, есть $p_{\text{loss}} \times (1 - p_{\text{USD}})^{-1}$.

Длина секретного ключа с учетом информации Евы выражается следующим образом. О всем сыром ключе длиной $1 - p_{\text{loss}}$, Ева знает информацию leak, полученную из открытого канала при коррекции ошибок (эта величина зависит как от наблюдаемой ошибки Q, так и от используемого легитимными пользователями метода коррекции ошибок). Также она знает всю информацию о части δp_{USD}, для которой безошибочное различение было успешным, и информацию C_1 о части $1 - \delta$, к которой не применялось безошибочное различение, но которая попала в ключ. Имеем

$$R_{\text{key}} = (1 - p_{\text{loss}})(1 - \text{leak}) - (1 - \delta)C_1 - \delta p_{\text{USD}}, \qquad (7)$$

что совпадает с формулой (11) в [9] (см. также [30], где эта формула приведена под номером (7) с дублированием аргументации).

Подчеркивается, что эта формула включает консервативную оценку сверху на информацию Евы, и она зависит только от наблюдаемых и вычисляемых на основе параметров протокола величин.

Перечислим вкратце основные ошибки, допущенные при выводе формулы (7):

1. Применение безошибочного различения к части посылок не является оптимальной стратегией, далее будут предложены более эффективные атаки.

2. Информацию перехватчика некорректно оценивать через пропускную способность за один шаг C_1, т.к. в других атаках он может совершать измерения, имея кодовую таблицу.

В следующих разделах эти тезисы разъяснены, и продемонстрированы атаки, при которых перехватчик имеет больше информации, т.е. при которых скорость генерации ключа должна быть ниже. Фактически это означает, что если пользоваться формулой (7), то часть ключа оказывается известной перехватчику, что, конечно, неприемлемо.

На рис.1 показана зависимость скорости генерации секретного ключа от расстояния между легитимными

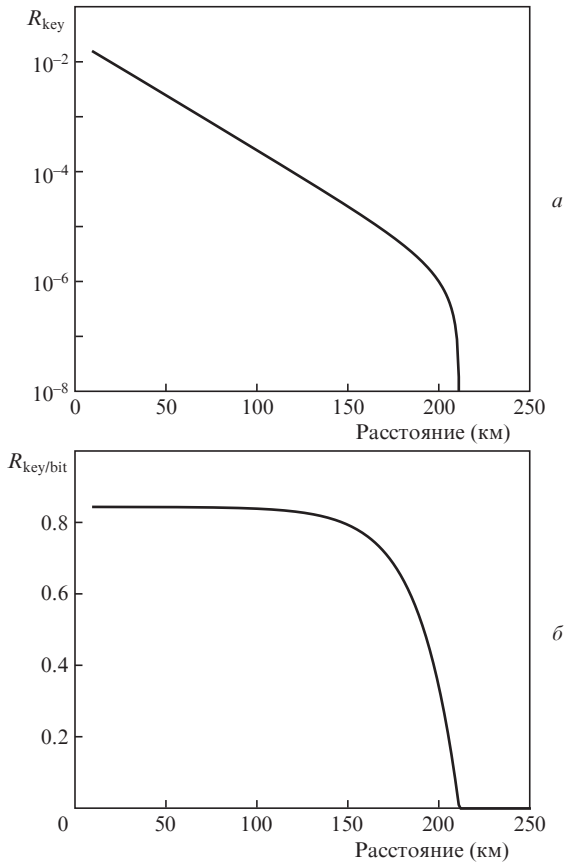

Рис.1. Зависимости скорости генерации секретного ключа от расстояния между легитимными пользователями для протокола на геометрически однородных состояниях с $N = 8$ состояниями, разделенными на $M = 4$ базиса (интенсивность $\mu = 0.4$ фотон./имп., фазовый сдвиг внутри базиса $\theta = \pi/4$) согласно формуле (7) (*а*), и в пересчете на один бит сырого ключа согласно формуле (8) (*б*). Затухание в линии связи $\kappa = 0.2$ дБ/км, ошибка нулевая.

пользователями, а также эта скорость в пересчете на один бит сырого ключа:

$$R_{\text{key/bit}} = \frac{R_{\text{key}}}{R_{\text{raw key}}} = \frac{(1-p_{\text{loss}})(1-\text{leak}) - (1-\delta)C_1 - \delta p_{\text{USD}}}{1-p_{\text{loss}}}. \qquad (8)$$

Зависимость, полученная по формуле (8), более наглядна на линейной шкале, поэтому в дальнейшем мы будем чаще сравнивать длины ключей именно для этого случая. Отметим, что формулы (7), (8) не содержат вероятности совпадения базисов $1/M$, однако при выборе оптимальных параметров протокола эти вероятности, конечно, должны учитываться.

4. Атака светоделителем, схема активного светоделителя

В этом разделе показано, что формула (7) оказывается ошибочной даже при применении перехватчиком концептуально самой простой атаки в условиях затухания: атаки светоделителем. Эта атака сводится к тому, что Ева моделирует потери в канале с помощью светоделителя, отводя себе часть состояния, а затем измеряет эту часть, зная базис. Также в этом разделе описана схема активного светоделителя, которая понадобится в дальнейшем для построения более эффективных атак.

Действие светоделителя на когерентное состояние $|\alpha\rangle$, где на втором входе находится вакуумное состояние, можно описать как

$$|\alpha\rangle_{\text{A}} \to |t\alpha\rangle_{\text{B}}|r\alpha\rangle_{\text{E}}, \qquad (9)$$

где r и t – показатели отражения и прохождения соответственно, $|r|^2 + |t|^2 = 1$. Чтобы Боб получил состояние с интенсивностью $\tilde{\mu}$, определяемое из (3), Еве нужно использовать коэффициент $t = \sqrt{\tilde{\mu}/\mu}$.

Далее Ева отправляет Бобу состояния $|t\alpha\rangle_{\text{B}}$ по каналу без потерь, и Боб получает в точности то, что ожидает. Состояния же $|r\alpha\rangle_{\text{E}}$ Ева сохраняет в своей квантовой памяти и измеряет их после объявления базисов и после раскрытия остальной информации (такой, как кодовая таблица при коррекции ошибок). Информация Евы $I_{\text{BS}}(\text{A}:\text{E})$ в этом случае дается величиной Холево [28, 31] состояний $\{|r\alpha_b^0\rangle_{\text{E}}, |r\alpha_b^1\rangle_{\text{E}}\}$ внутри базиса:

$$I_{\text{BS}}(\text{A}:\text{E}) = h_2\left(\frac{1-|{}_{\text{E}}\langle r\alpha_b^0|r\alpha_b^1\rangle_{\text{E}}|}{2}\right) = h_2\left\{\frac{1-\exp[-(1-\cos\theta)(\mu-\tilde{\mu})]}{2}\right\}.$$

Такая информация перехватчика дает скорость генерации ключа в пересчете на одну посылку

$$R_{\text{key/bit, BS}} = 1 - I_{\text{BS}}(\text{A}:\text{E}) = 1 - h_2\left\{\frac{1-\exp[-(1-\cos\theta)(\mu-\tilde{\mu})]}{2}\right\}. \qquad (10)$$

При большой длине линии связи величина $\tilde{\mu} \to 0$, и информация Евы стремится к величине Холево исходных состояний, поэтому при такой атаке перехватчик не получает полной информации даже при очень больших потерях в канале.

На рис.2 показаны скорости генерации секретного ключа в пересчете на один бит сырого ключа для формулы (8) и для атаки светоделителем согласно (10). Можно увидеть, что на длинах линии связи 12–172 км атака светоделителем работает эффективно и скорость генерации ключа оказывается ниже полученной по формуле (8). Ошибка, приведшая к завышению скорости генерации ключа в (8), уже упоминалась выше: это использование пропускной способности за один шаг C_1 вместо величины Холево для оценки информации перехватчика. Такое использование оправданно, когда перехватчик стоит перед необходимостью измерить состояния, не имея кодовой таблицы [29] (см. также [32]), однако в случае атаки светоделителем такой необходимости нет, и перехватчик может подождать объявления кодовых слов. Так, при длине линии связи 90 км (а это потери в 18 дБ, как в [21]), завышение скорости генерации ключа составляет около 20%, что говорит о том, что перехватчику известно более 17% ключа.

Следует отметить, что если в (8) заменить пропускную способность за один шаг C_1 величиной Холево состояний внутри базиса, то атака светоделителем уже не приведет к потере секретности, т. к. ключ, полученный по формуле

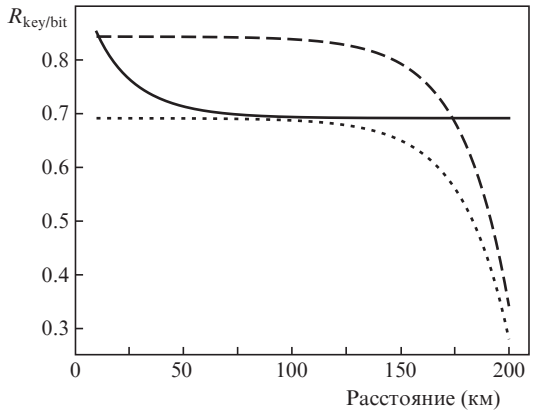

Рис.2. Зависимости скорости генерации секретного ключа от расстояния между легитимными пользователями при атаке светоделителем, полученные по формуле (10) (сплошная кривая), по формуле (8) (штриховая кривая), а также по формуле (11) (пунктир). Параметры протокола: $N = 8$ состояний ($M = 4$ базиса), интенсивность $\mu = 0.4$ фотон./имп., фазовый сдвиг внутри базиса $\theta = \pi/4$. Затухание в линии связи $\kappa = 0.2$ дБ/км, ошибка нулевая.

$$R'_{\text{key/bit}} = \frac{(1-p_{\text{loss}})(1-\text{leak}) - (1-\delta)\chi - \delta p_{\text{USD}}}{1-p_{\text{loss}}}, \qquad (11)$$

где величина Холево χ равновероятных состояний $\{|\alpha_b^0\rangle, |\alpha_b^1\rangle\}$

$$\chi(\{|\alpha_b^0\rangle, |\alpha_b^1\rangle\}) = h_2\left(\frac{1-|\langle\alpha_b^0|\alpha_b^1\rangle|}{2}\right),$$

оказывается меньшей длины, чем секретный ключ, полученный по формуле (10) (рис.2). В дальнейшем, однако, будут описаны более эффективные атаки, для которых формула (11) также оказывается неверной.

Опишем здесь схему активного светоделителя (рис.3), которая уже применялась для ряда атак [33, 34] и будет использоваться в нашей работе. Суть этой технологии подслушивания в том, что Ева не просто сохраняет отведенные светоделителем состояния в своей квантовой памяти, а производит над ними преобразование и, в зависимости от его результата, блокирует оставшееся состояние или отправляет его на принимающую сторону. Такая схема позволяет добиться большей гибкости: Ева может отправлять Бобу состояния только в тех позициях, в которых, как она уверена, можно получить много информации из своих состояний и блокировать состояния в других случаях. Также важным преимуществом такой схемы является то, что Ева производит преобразование над частью состояния, которая не достанется Бобу, поэтому она может вносить туда какие угодно изменения, и это не приведет к ошибке на принимающей стороне.

Условие применимости атаки активным светоделителем состоит в том, что детектор Боба должен срабатывать с такой же вероятностью, как и в отсутствие атаки. Если Ева отправляет на принимающую сторону состояния с интенсивностью $|t|^2\mu$, то это накладывает на вероятность успеха $p_{\text{succ}}^{\text{E}}$ ее преобразования (т.е. на вероятность отправки состояний) следующие требования:

$$\tfrac{1}{2}\{1-\exp[-\tfrac{1}{2}(1-\cos\theta)\tilde{\mu}]\} = \tfrac{1}{2}p_{\text{succ}}^{\text{E}}\{1-\exp[-\tfrac{1}{2}(1-\cos\theta)\,|t|^2\mu]\}. \qquad (12)$$

Левая часть этого выражения соответствует ожидаемой вероятности (5) получения определенного результата измерения внутри базиса в отсутствие перехватчика. Правая же часть соответствует тому, что перехватчик с вероятностью $p_{\text{succ}}^{\text{E}}$ отправляет на принимающую сторону импульсы с интенсивностью $|t|^2\mu$, и для этих импульсов на принимающей стороне фиксируется определенный результат измерения.

Отметим, что приведенная здесь схема активного светоделителя имеет недостаток: в случае неудачи происходит блокировка оставшегося состояния, тогда как эффективнее применять преобразование над всем состоянием, чтобы в случае удачи оно выдавало в том числе состояние для отправки Бобу, а при неудаче давало на выходе всегда одно и то же состояние. Тогда соображения унитарности позволят повысить общую вероятность успеха (см., напр., [35]). Тем не менее такой прием усложнит математическое описание приведенных атак и сделает менее ясной их физическую интерпретацию. Однако, поскольку оптимизация атак не является целью настоящей работы, в дальнейшем мы будем рассматривать описанную здесь концептуально простую схему активного светоделителя.

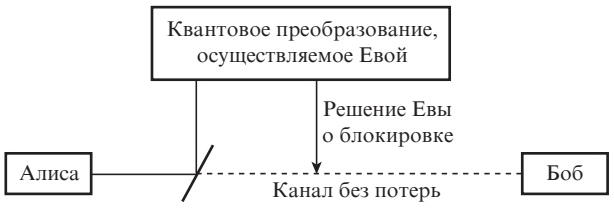

Рис.3. Схема атаки активным светоделителем.

5. Вариант атаки расщеплением по числу фотонов

В этом разделе будет описана атака, наиболее ярко демонстрирующая ошибочность формулы (7) для длины секретного ключа.

Атака расщеплением по числу фотонов (photon number splitting attack, PNS-атака) разрабатывалась для протокола BB84, и она подробно описана в [15]. Суть этой атаки в том, что если легитимные пользователи используют когерентные состояния с фазовой рандомизацией

$$\rho_\mu = \int_0^{2\pi} |\sqrt{\mu}\exp(\mathrm{i}\phi)\rangle\langle\sqrt{\mu}\exp(\mathrm{i}\phi)|\frac{\mathrm{d}\phi}{2\pi} = \exp(-\mu)\sum_{n=0}^{+\infty}\frac{\mu^n}{n!}|n\rangle\langle n|,$$

то перехватчик может неразрушающим образом измерить число фотонов в импульсе, а затем, если фотонов более одного, отвести часть из них в свою квантовую память. После раскрытия базисов перехватчик проводит измерение в нужном базисе и получает всю информацию.

Здесь важно отметить, что рассуждения, приведшие к формулам (7) и (8) для длины секретного ключа, никак не зависят от фазового сдвига θ между состояниями внутри базиса, используемого в протоколе на геометрически однородных состояниях. Поэтому, если эти рассуждения верны, формулы должны быть справедливы для любого значения θ. Более того, несложно провести численную

оптимизацию длины ключа согласно этим формулам для произвольной длины линии связи, в том числе приняв во внимание вероятность несовпадения базисов, и увидеть, что оптимальным значением фазового сдвига является $\theta = \pi$. Это следует и из таких рассуждений: в формуле (7) длина ключа зависит от скалярного соотношения между векторами внутри базиса и от вероятности безошибочного различения состояний. Если фиксировать число состояний и скалярное произведение внутри базиса, то минимальная вероятность успеха при безошибочном различении состояний будет достигаться на состояниях с малой интенсивностью и с фазовым сдвигом π внутри базиса. При этом вероятность определенного исхода на приемной стороне, как видно из (4) и (5), зависит лишь от скалярного произведения. Поэтому оптимальным фазовым сдвигом внутри базиса, согласно (7), является сдвиг π. Вся аргументация, приведшая к формуле (7), оказывается справедливой и для этого случая: Ева по-прежнему имеет ограниченную вероятность успеха для безошибочного различения состояний (которая не зависит от θ, а только от интенсивности μ и числа N когерентных состояний); кроме того, информация Евы ограничена из-за неортогональности состояний внутри базиса (хотя выше и было показано, что использование величины Холево вместо пропускной способности за один шаг будет более оправданным). Фазовый сдвиг θ будет оказывать влияние на величину C_1, но в остальном формула для скорости генерации ключа должна оставаться верной.

Покажем, что использование фазового сдвига $\theta = \pi$ приводит к катастрофической потере секретности.

На первый взгляд, PNS-атака неприменима к протоколу, использующему чистые состояния без фазовой рандомизации, т. к. измерение числа фотонов приведет к потере информации о фазе. Однако покажем, что схема активного светоделителя, описанная в разд.4, позволяет обойти эту проблему. Пусть Ева оставила часть состояний с интенсивностью $|t|^2\mu$ Бобу, а себе отвела состояния с интенсивностью $|r|^2\mu$. Над своими состояниями Ева может совершать любые разрешенные квантовой механикой преобразования. В частности, Ева может провести общую фазовую рандомизацию пары из опорного и информационного состояний $|r\alpha\rangle|r\alpha\exp(\mathrm{i}\gamma)\rangle$ (см. (2)), после которой оно будет иметь вид [15]

$$\rho_\gamma^{\mathrm{E}} = \int_0^{2\pi} |r\alpha\exp(\mathrm{i}\phi)\rangle\langle r\alpha\exp(\mathrm{i}\phi)| \otimes |r\alpha\exp[\mathrm{i}(\phi+\gamma)]\rangle\langle r\alpha\exp[\mathrm{i}(\phi+\gamma)]| \frac{\mathrm{d}\phi}{2\pi} = \exp(-2|r|^2\mu)\sum_{n=0}^{+\infty}\frac{(2|r|^2\mu)^n}{n!}|\psi_n(\gamma)\rangle\langle\psi_n(\gamma)|. \qquad (13)$$

Это смесь состояний

$$|\psi_n(\gamma)\rangle = \sum_{m=0}^{n}\sqrt{\frac{C_n^m}{2^n}}\exp(\mathrm{i}m\gamma)\,|n-m\rangle|m\rangle \qquad (14)$$

с определенным числом фотонов n, которое перехватчик может измерить, не внеся возмущение в состояния $|\psi_n(\gamma)\rangle$. Фактически перехватчик измеряет суммарное число фотонов в двух модах – опорной и информационной, но не число фотонов в каждой из них. При наличии хотя бы одного фотона перехватчик сохраняет его в своей квантовой памяти, а оставшееся после светоделителя состояние интенсивности $|t|^2\mu$ пересылает Бобу. Если же число фотонов нулевое, перехватчик блокирует импульс, направлявшийся к Бобу. После оглашения базиса перехватчик стоит перед задачей извлечения информации из однофотонных состояний $\{|\psi_1(2\pi k(b)/N)\rangle, |\psi_1(2\pi k(b)/N+\theta)\rangle\}$ внутри одного известного базиса (см. (1)), которые, как легко видеть, взаимно ортогональны при фазовом сдвиге $\theta = \pi$:

$$|\psi_1(2\pi k(b)/N)\rangle = \frac{1}{\sqrt{2}}(|1\rangle|0\rangle + \exp[\mathrm{i}2\pi k(b)/N]\,|0\rangle|1\rangle),$$

$$|\psi_1(2\pi k(b)/N+\pi)\rangle = \frac{1}{\sqrt{2}}(|1\rangle|0\rangle + \exp[\mathrm{i}2\pi k(b)/N+\pi]\,|0\rangle|1\rangle).$$

Таким образом, при наличии хотя бы одного фотона в своем состоянии (13), что происходит с вероятностью $p_{\mathrm{succ}}^{\mathrm{E}} = 1 - \exp(-2|r|^2\mu)$, перехватчик имеет всю информацию. Условие применимости атаки (12), как отмечалось выше, состоит в том, что вносимые перехватчиком потери равны ожидаемым.

Тут важно отметить, что условие (12) не зависит от общего числа состояний N, т. е. увеличение числа состояний мешает применению USD-атаки, но не мешает проведению описанной здесь модификации PNS-атаки. Эффективность предложенной атаки возникает за счет того, что перехватчик не пробует совершать сложных действий, таких как различение всех N состояний. Он только отображает эти состояния на взаимно ортогональные в каждом базисе пары, что и происходит при фазовой рандомизации и блокировании посылок, в которых число фотонов равно нулю. Такая операция имеет существенно более высокую вероятность успеха, которая не зависит от числа состояний. Следует также отметить, что описанная атака, в отличие от USD-атаки, существенно использует информацию о базисе, объявляемую позже, вследствие чего во многом и достигается ее высокая эффективность. То, что такая атака была пропущена при выводе формулы генерации секретного ключа, возможно, вызвано грубой ошибкой в работах [10, 30], где PNS-атака названа частным случаем USD-атаки. Это не так, и в этом разделе показано, что PNS-атака мощнее за счет использования объявляемой впоследствии информации о базисах, из-за чего на момент атаки перехватчик не стоит перед необходимостью различать все N состояний.

На рис.4 приведены оптимальная интенсивность для каждой длины линии связи при фазовом сдвиге внутри базиса $\theta = \pi$ (при оптимальном выборе числа базисов M) согласно формуле (7) с учетом вероятности совпадения базисов, а также критическая интенсивность, при которой протокол перестает быть секретным в случае применения описанной здесь PNS-атаки. Видно, что, начиная с длины 45 км, при оптимальной с точки зрения (7) интенсивности сигнала Ева получает всю информацию о ключе.

Основной вывод этого раздела заключается в том, что при фазовом сдвиге $\theta = \pi$ формула (7) оказывается грубо неверной. Для других фазовых сдвигов рассмотренная здесь атака оказывается менее эффективной, т. к. при отведении лишь одного фотона перехватчик имеет неполную информацию из-за неортогональности однофотонных состояний вида (14). Тем не менее перехватчик может оставлять себе больше одного фотона, что способно также увеличить эффективность предложенной атаки. Пол-

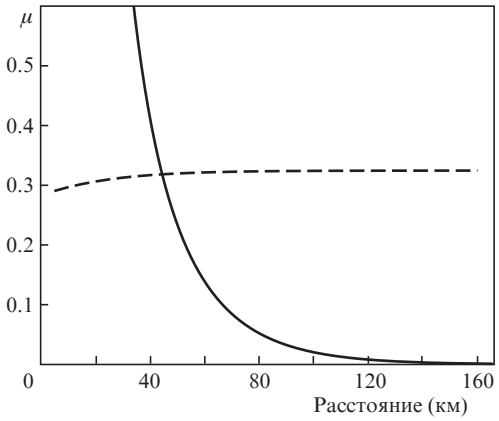

Рис.4. Зависимости от длины линии связи критической интенсивности μ, при которой перехватчику известен весь ключ, в случае применения противником модифицированной PNS-атаки (сплошная кривая), а также оптимальной интенсивности согласно (7) (штриховая кривая). Фазовый сдвиг внутри базиса $\theta = \pi$, затухание в линии связи $\kappa = 0.2$ дБ/км, ошибка нулевая.

ный анализ построенной атаки выходит за рамки настоящей работы, цель которой – продемонстрировать наиболее яркие примеры ошибочности формулы (7). В дальнейших разделах будут рассматриваться значения $\theta = \pi/M$, соответствующие работе [9], и атаки для них.

6. Атака усилением состояний

В этом разделе мы рассмотрим атаку, которая демонстрирует существенное завышение ключа в практических условиях [21].

Согласно формуле (7), если вероятность потерь в канале меньше вероятности неудачи при безошибочном различении входных состояний, Ева уже не может применять безошибочное различение к каждой позиции. Поэтому USD-атака невозможна на длинах линии связи меньше критической, когда Алиса и Боб ожидают небольших потерь. Однако в (7) предполагается, что на таких небольших длинах оптимальной стратегией для перехватчика является применение безошибочного различения к доле δ посылок, а для оставшейся части – использование других стратегий подслушивания.

В работах [34, 36, 37] предлагается другой подход к действиям перехватчика на длинах линии связи, при которых USD-атака невозможна. Ева может не применять безошибочное различение вероятностным образом, а сделать его лишь «частично», т.е. увеличить различимость входных состояний, не сделав их полностью ортогональными (см. также [38]). Такая операция имеет более высокую вероятность успеха, поэтому допустима и в условиях небольшого затухания в канале. В этом разделе будет предложена модифицированная версия атаки из [37], более простая и эффективная.

Пусть A – матрица, столбцами которой являются коэффициенты каждого вектора $\{|\alpha_j\rangle\}_j$ при разложении по некоторому ортонормированному базису. В силу линейной независимости состояний существует обратная матрица A^{-1}. Несложно видеть, что векторы $\{A^{-1}|\alpha_j\rangle\}_j$ являются взаимно ортогональными и имеют единичную длину. Далее рассмотрим набор $\{|\beta_j\rangle\}_j$ также симметричных когерентных состояний, имеющих интенсивность $\mu_{\rm B}$, и соответствующую матрицу из коэффициентов B. Очевидно, что

$$|\beta_j\rangle = BA^{-1}|\alpha_j\rangle,$$

таким образом, преобразование BA^{-1}, в случае, когда $\mu_{\rm B} > \mu$, увеличивает интенсивность каждого состояния, сохраняя остальные их свойства. Операторы Крауса для квантового канала, соответствующие успеху (succ) и неудаче (fail), можно определить следующим образом:

$$M_{\rm succ} = \frac{BA^{-1}}{\sqrt{\lambda}}, \quad M_{\rm fail} = \sqrt{1 - M_{\rm succ}^{\dagger} M_{\rm succ}}, \tag{15}$$

где λ – максимальное собственное значение матрицы $(BA^{-1})^{\dagger}BA^{-1}$. Такое квантовое преобразование в случае успеха увеличивает интенсивность всех когерентных состояний.

Атака на основе построенного преобразования устроена просто: Ева проводит преобразование (15) и блокирует состояния в случае неудачи, в случае же успеха отводит их часть в свою квантовую память, а часть отправляет Бобу по каналу без потерь. У атаки всего два параметра: интенсивность $\mu_{\rm B}$ состояний на выходе преобразования (15), а также интенсивность состояния, которое остается у Евы в случае успеха. Несложно численным образом найти значения этих параметров для каждой длины канала, которые давали бы максимум информации перехватчику. Информация перехватчика о ключе дается, как и в случае атаки светоделителем, величиной Холево его состояний внутри базиса.

На рис.5 представлены зависимости длины ключа от длины линии связи для протокола с $N = 8$ состояниями с интенсивностью $\mu = 0.4$, разделенными на $M = 4$ базиса. Видно, что, например, при длине линии связи 165 км формула (8) завышает длину ключа примерно на 64%; это означает, что примерно 39% ключа известны перехватчику. Также показано, что, в отличие от атаки светоделителем, даже если заменить величину C_1 в (8) на величину Холево состояний, все равно будет иметь место завышение длины секретного ключа.

Кроме того, имеет смысл расписать результаты применения атаки для практических параметров, приведенных в [21]: так, на городской линии ПАО «Ростелеком» (затухание 18 дБ, исходная интенсивность 0.5 фотон./ имп., наблюдаемая ошибка 6%) завышение длины ключа пре-

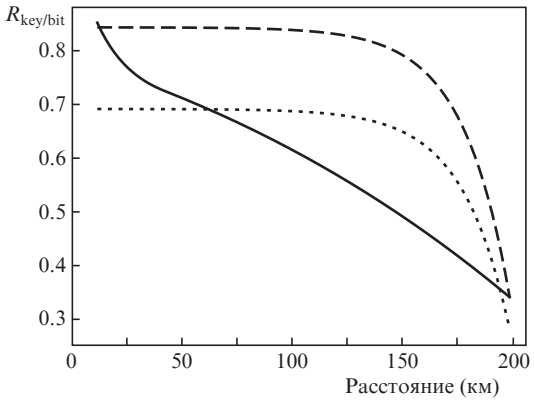

Рис.5. Зависимость скорости генерации секретного ключа от расстояния между легитимными пользователями при атаке усилением состояний (сплошная кривая), а также зависимости, полученные по формулам (8) (штриховая кривая) и (11) (пунктир). Параметры протокола: $N = 8$ состояний ($M = 4$ базиса), интенсивность $\mu = 0.4$ фотон./имп., фазовый сдвиг внутри базиса $\theta = \pi/4$. Затухание в линии связи $\kappa = 0.2$ дБ/км, ошибка нулевая.

вышает 88%, т.е. перехватчику известно более 46% ключа. Такое большое завышение вызвано тем, что при наличии ошибки перехватчик получает сравнительно большую информацию из открытого канала во время процедуры коррекции ошибок, и различие между длинами ключей становится еще более существенным. Отметим, что здесь мы рассматривали худший вариант для перехватчика, когда при наблюдаемой ошибке Q он получает лишь $h_2(Q)$ информации, что соответствует использованию кодов с идеальной эффективностью. При практически доступных методах коррекции ошибок перехватчик имеет больше информации [9, 30], и длина ключа завышается еще сильнее.

Таким образом, преобразование мягкой фильтрации [35, 36, 39], очередная версия которого была здесь продемонстрирована, более эффективно для атаки и получения информации с заданной вероятностью успеха, чем вероятностное применение безошибочного различения состояний, которое использовалось при выводе (7).

Отметим кроме того, что атака, предложенная в [37], если ее применить к тем же входным параметрам, также демонстрирует завышение длины ключа в формуле (7).

7. Атака различением битов ключа

В этом разделе будет рассмотрена атака, которая показывает, что увеличение числа базисов не обязательно существенно помогает легитимным пользователям обезопасить себя от перехватчика в условиях затухания. В этой атаке перехватчик не пытается различить все передаваемые состояния, как это происходит при USD-атаке и (в более мягкой форме) при атаке усилением состояний, описанной в разд.6. Это действие достаточно «дорогое» для перехватчика, поскольку оно имеет малую вероятность успеха при большом числе состояний. Однако важно отметить, что при проведении атаки конечной целью перехватчика является знание битов ключа, а не того, какое из состояний отправлено по каналу. Здесь мы рассмотрим обобщение безошибочного различения состояний, которое имеет значительно более высокую вероятность успеха, однако идентифицирует не состояние, а лишь его принадлежность к классу состояний. Это позволяет провести различение нулей и единиц в сыром ключе со значительно возросшей вероятностью успеха, что в конечном итоге дает перехватчику всю информацию.

Рассмотрим сначала подробнее измерение, соответствующее безошибочному различению состояний $\{|\alpha_j\rangle\}_j$. Каждый элемент наблюдаемой, соответствующий удачному исходу k, можно записать в виде [40]

$$M_k = c\,|\psi_k^{\perp}\rangle\langle\psi_k^{\perp}| = c(I - P_k), \tag{16}$$

где $|\psi_k^{\perp}\rangle$ – вектор, ортогональный всем векторам $\{|\alpha_j\rangle\}_{j,j\neq k}$, а P_k – проектор на подпространство, натянутое на векторы $\{|\alpha_j\rangle\}_{j,j\neq k}$. Коэффициент c определяется требованием неотрицательности оператора $M_?$, соответствующего неудаче:

$$\lambda_{\min}(M_?) = \lambda_{\min}\left(1 - \sum_{k=1}^{N} M_k\right) = 0. \tag{17}$$

Легко видеть, что вероятность ошибки при таком измерении нулевая:

$$p(k|j) = \mathrm{Tr} M_k\,|\alpha_j\rangle\langle\alpha_j| = c\,|\langle\alpha_j|\psi_k^{\perp}\rangle|^2 = c\,|\langle\alpha_j|\psi_k^{\perp}\rangle|^2\delta_{jk},$$

а вероятность удачного результата определяется требованием (17) и вытекающим из него значением коэффициента c (одинакового для всех операторов M_k в симметричном случае).

Схожим образом можно определить наблюдаемую с тремя элементами, $\{M_0, M_1, M_?\}$, которая не идентифицирует вектор полностью, а лишь дает информацию о его принадлежности к набору векторов, соответствующих нулю или единице в сыром ключе:

$$M_0 = c(I - P_1),\ \ M_1 = c(I - P_0),\ \ M_? = I - M_0 - M_1, \tag{18}$$

где P_i – проектор на подпространство, натянутое на векторы $\{|\alpha_b^i\rangle\}_b$, соответствующие нулю или единице в сыром ключе. Несложно убедиться, что исход 0 такого измерения выпадает только на состояниях, соответствующих нулям в сыром ключе, а исход 1 – только на состояниях, соответствующих единицам. Вероятность неудачи при этом может быть значительно ниже, чем для преобразования (16), поскольку измерение (18) дает, вообще говоря, меньше информации о самом состоянии. Но для атаки в квантовой криптографии оно оказывается очень полезным из-за более высокой вероятности успеха, которую несложно вычислить, пользуясь конкретным ортонормированным базисом в пространстве, натянутом на симметричные когерентные состояния, и коэффициентами разложения по нему из [12].

Фактически это преобразование соответствует безошибочному различению двух состояний,

$$\frac{1}{M}\sum_b |\alpha_b^0\rangle\langle\alpha_b^0|,\quad \frac{1}{M}\sum_b |\alpha_b^1\rangle\langle\alpha_b^1|,$$

которые соответствуют отправке битов ключей 0 и 1 соответственно, когда базис b неизвестен. Методы для безошибочного различения смешанных состояний хорошо известны [41, 42].

Сразу рассмотрим небольшую модификацию измерения, которая делает соответствующую атаку более эффективной. Поскольку Ева впоследствии получает информацию о базисе, ей не обязательно различать именно нули и единицы сырого ключа. Еве достаточно добиться лишь различения между двумя группами состояний, где состояния каждого базиса принадлежат разным группам. К примеру, для восьми состояний с фазовым сдвигом внутри базиса $\theta = \pi/4$ это могут быть группы из номеров состояний $G_a = \{0, 3, 4, 7\}$ и $G_b = \{1, 2, 5, 6\}$. Тогда принадлежность состояния группе a будет означать вектор с индексом 0, если используется первый базис; вектор 3, если используется второй базис, и так далее: знание группы и базиса однозначно идентифицирует состояние, а значит, и бит сырого ключа. При этом из-за геометрии состояний различить группы G_a и G_b можно с большей вероятностью успеха, чем группы $G_0 = \{0, 2, 4, 6\}$ и $G_1 = \{1,3,5,7\}$, соответствующие битам 0 и 1 ключа.

Атака на основе предложенного преобразования строится по схеме активного светоделителя (см. разд.4). Ева отводит себе часть состояния с интенсивностью $|r|^2\mu$ и совершает над ней различение двух групп состояний. Если это различение прошло успешно, оставшаяся часть состояния с интенсивностью $|t|^2\mu$ отправляется Бобу,

иначе она блокируется. Фактически у атаки только один параметр – отведенная часть состояния, и при известном затухании атака возможна, начиная с некоторого критического значения интенсивности. Если атака возможна, Ева получает весь секретный ключ.

На рис.6 для каждой длины линии связи показаны оптимальные интенсивности, полученные по формуле (7), и критические значения интенсивности, при которых перехватчик знает весь ключ, проводя описанную в этом разделе атаку. Число состояний и конфигурация фиксированы. Видно, что для длины линии связи при использовании четырех базисов с фазовым сдвигом $\theta = \pi/4$ критическая интенсивность становится больше оптимальной, начиная с расстояния примерно 210 км, а при использовании восьми базисов с фазовым сдвигом $\theta = \pi/8$ это происходит, начиная примерно со 130 км. Для сравнения показаны критические интенсивности при применении USD-атаки, и они, как и ожидалось, оказываются выше оптимальных. Таким образом, протокол фокусируется на USD-атаке и предлагает меры для противодействия ей, тогда как при использовании большого числа базисов стойкость протокола к другим атакам не гарантируется.

При этом следует отметить, что для ряда длин атака безошибочным различением состояний более эффективна (что видно и на рис.6,*а*, на длине до 90 км). Этот, на первый взгляд, неожиданный факт обусловлен тем, что

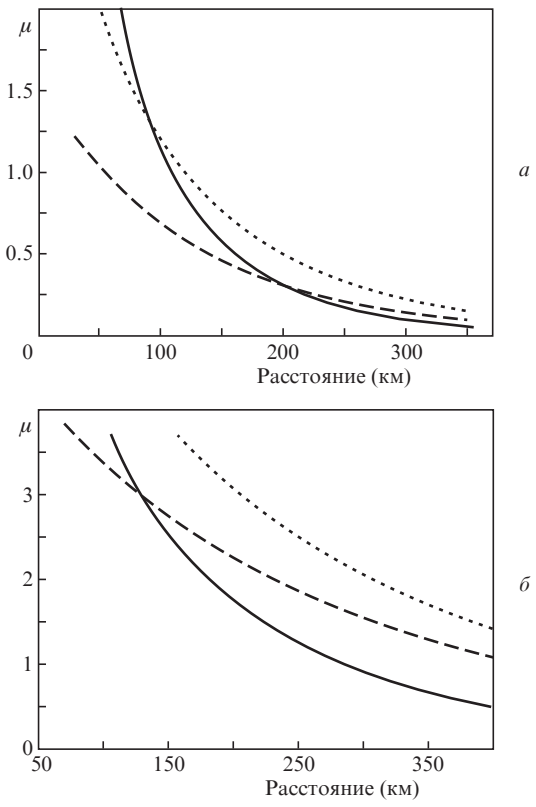

Рис.6. Зависимости критической интенсивности μ, при которой перехватчику известен весь ключ, от длины линии связи при применении противником атаки различением битов ключа (сплошные кривые) и оптимальной интенсивности согласно (7) (штриховые кривые), а также критической интенсивности, при которой перехватчику известен весь ключ в случае применения USD-атаки (пунктир) при $M = 4$ базиса, фазовый сдвиг внутри базиса $\theta = \pi/4$ (*а*) и $M = 8$ базисов, фазовый сдвиг внутри базиса $\theta = \pi/8$ (*б*). Затухание в линии связи $\kappa = 0.2$ дБ/км, ошибка нулевая.

при USD-атаке Ева получает полную информацию о сигнале и может приготовить корректное состояние с большой интенсивностью, тем самым спровоцировав срабатывание детектора в удобной для нее позиции. Ева лишена этой возможности в случае применения атаки, описанной в этом разделе, поэтому при некоторых наборах параметров она оказывается менее эффективной.

Следует также отметить техническую простоту этой атаки для перехватчика: она не требует наличия у него долговременной квантовой памяти. Еве нужно хранить лишь классический результат измерения, который дает ей информацию о бите ключа после объявления базисов.

8. Заключение

В настоящей работе был рассмотрен набор атак, которые демонстрируют завышение скорости генерации секретного ключа в протоколе на геометрически однородных когерентных состояниях. Для атаки светоделителем и атаки усилением состояний, при которых Ева получает неполную информацию, было проведено сравнение длины секретного ключа, рассчитанной по формуле (8), и длины секретного ключа, получающейся при проведении атаки. Для модифицированной PNS-атаки и атаки различением битов ключа, при которых Ева получает полную информацию, было проведено сравнение критической интенсивности для каждой длины линии связи с оптимальной интенсивностью для той же конфигурации состояний, полученной в соответствии с (7). Все атаки в тех или иных условиях обеспечивают завышение длины секретного ключа в формуле (7); это означает, что ключ, распределенный по соответствующему протоколу, не является секретным. Таким образом показана ошибочность формулы (7) для скорости генерации секретного ключа.

Отметим, что большинство приведенных здесь атак имеет некоторые недостатки, устранение которых сделает атаки более эффективными, но затруднит их подробное описание и анализ. Целью работы было описание максимально простых атак, демонстрирующих ошибочность формулы (7), поэтому максимизации их эффективности уделялось мало внимания. Так, совсем не рассматривались атаки, которые вносят ошибку в передаваемые состояния, хотя это может существенно увеличить информацию перехватчика. Рассматривалась идеальная работа оборудования легитимных пользователей: полная эффективность детекторов, отсутствие темновых срабатываний детекторов и т. д. По всей видимости, оптимальная атака на данный протокол квантовой криптографии будет сочетать свойства нескольких приведенных здесь атак и будет существенно более сложной. (См. также [43], где была построена еще одна атака, использующая более сложные гетеродинные измерения и демонстрирующая, что увеличение числа базисов не обязательно позволяет бороться с противником при наличии затухания.)

Протокол на геометрически однородных состояниях использует большое число состояний, что затрудняет полное доказательство его криптографической стойкости, и заявления авторов о его доказуемой стойкости [10, 44] неверны. На первый взгляд, сложная конфигурация состояний усложняет и атаки, но в нашей работе показано, что, наоборот, такая конфигурация состояний открывает перед перехватчиком множество новых возможностей.

Основным результатом работы является вывод о том, что использование интуитивных формул для длины секретного ключа, основанных на предположениях о применении перехватчиком тех или иных атак, является очень рискованным и может привести к компрометации всей системы: велики шансы, что некоторые эффективные действия перехватчика не были учтены при рассмотрении известных атак. Ключевым преимуществом квантовой криптографии является возможность строгого доказательство криптографической стойкости против всех действий противника (см. напр., [4–7, 45, 46]).

Исследование выполнено за счет Российского научного фонда (проект № 20-71-10072).

1. Bennett Ch.H., Brassard G. *Proc. Int. Conf. Computers, Systems & Signal Processing* (Bangalore, India, 1984, p. 175).
2. Ekert A.K. *Phys. Rev. Lett*., **67** (6), 661 (1991).
3. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys*., **74** (1), 145 (2002).
4. Mayers D. *J. ACM*, **48** (3), 351 (2001).
5. Shor P.W., Preskill J. *Phys. Rev. Lett*., **85** (2), 441 (2000).
6. Koashi M. *New J. Phys.*, **11** (4), 045018 (2009).
7. Renner R., Gisin N., Kraus B. *Phys. Rev. A*, **72** (1), 012332 (2005).
8. Молотков С.Н. *Письма в ЖЭТФ*, **95** (6), 361 (2012) [*JETP Lett*., **95** (6), 332 (2012)].
9. Молотков С.Н. *Письма в ЖЭТФ*, **101** (8), 637 (2015) [*JETP Lett*., **101** (8), 579 (2015)].
10. Балыгин К.А., Зайцев В.И., Климов А.Н., Климов А.И., Кулик С.П., Молотков С.Н. *Письма в ЖЭТФ*, **105** (9), 570 (2017)) [*JETP Lett*., **105** (9), 606 (2017)].
11. Dušek M., Jahma M., Lütkenhaus N. *Phys. Rev. A*, **62** (2), 022306 (2000).
12. Chefles A., Barnett S.M. *Phys. Lett. A*, **250** (4–6), 223 (1998).
13. Yuen H.P. ArXiv preprint quant-ph/0311061 (2003).
14. Barbosa G.A., Corndorf E., Kumar P., Yuen H.P. *Phys. Rev. Lett*., **90** (22), 227901 (2003).
15. Acin A., Gisin N., Scarani V. *Phys. Rev. A*, **69** (1), 012309 (2004).
16. Hirota O., Sohma M., Fuse M., Kato K. *Phys. Rev. A*, **72** (2), 022335 (2005).
17. Аванесов А.С., Кронберг Д.А. *Квантовая электроника*, **49** (10), 974 (2019) [*Quantum Electron*., **49** (10), 974 (2019)].
18. Аванесов А.С., Кронберг Д.А. *Квантовая электроника*, **50** (5), 454 (2020) [*Quantum Electron*., **50** (5), 454 (2020)].
19. Futami F., Guan K., Gripp J., Kato K., Tanizawa K., Chandrasekhar S., Winzer P. *Opt. Express*, **25** (26), 33338 (2017).
20. Втюрина А.Г., Елисеев В.Л., Жиляев А.Е., Николаева А.С., Сергеев В.Н., Уривский А.В. *Докл. Томского гос.ун-та систем управления и радиоэлектроники*, **21** (2). 15 (2018).
21. Борисова А.В., Жиляев А.Е., Алфёров С.В., Елисеев В.Л., Кармазиков Ю.В., Климов А.Н., Балыгин К. А. *Вестник Российского нового университета. Сер. Сложные системы: модели, анализ и управление*, № 4, 100 (2019).
22. Ivanovic I.D. *Phys. Lett. A*, **123** (6), 257 (1987).
23. Peres A. *Phys. Lett. A*, **128** (1–2), 19 (1988).
24. Kronberg D.A. *Математические вопросы криптографии*, **8** (2), 77 (2017).
25. Kiktenko E.O., Malyshev A.O., Bozhedarov A.A., Pozhar N.O., Anufriev M.N., Fedorov A.K. *J. Russ. Laser Res.*, **39** (6), 558 (2018).
26. Трушечкин А.С. *Квантовая электроника*, **50** (5), 426 (2020) [*Quantum Electron*., **50** (5), 426 (2020)].
27. Devetak I., Winter A. *Proc. Royal Soc. A: Mathemat., Phys. Eng. Sci*., **461** (2053), 207 (2005).
28. Холево А.С. *Квантовые системы, каналы, информация* (М.: МЦНМО, 2010, с. 327).
29. Кронберг Д.А., Молотков С.Н. *Письма в ЖЭТФ*, **100** (4), 305 (2014) [*JETP Lett*., **100** (4), 279 (2014)].
30. Балыгин К.А., Климов А.Н., Кулик С.П., Молотков С.Н. *Письма в ЖЭТФ*, **104** (5), 349 (2016) [*JETP Lett*., **104** (5), 341 (2016)].
31. Холево А.С. *Успехи мат. наук*, **53** (324), 193 (1998).
32. Sasaki M., Kato K., Izutsu M., Hirota O. *Phys. Rev. A*, **58** (1), 146 (1998).
33. Кронберг Д.А., Киктенко Е.О., Федоров А.К., Курочкин Ю.В. *Квантовая электроника*, **47** (2), 163 (2017) [*Quantum Electron*., **47** (2), 163 (2017)].
34. Avanesov A.S., Kronberg D.A., Pechen A.N. *P-Adic Numbers, Ultrametric Analysis, and Applications*, **10** (3), 222 (2018).
35. Kronberg D.A., Nikolaeva A.S., Kurochkin Y.V., Fedorov A.K. *Phys. Rev. A*, **101** (3), 032334 (2020).
36. Kronberg D.A. *Laser Phys*., **24** (2), 025202 (2014).
37. Kronberg D.A. *Lobachevskii J. Mathem*., **41** (12), 2332 (2020).
38. Кронберг Д.А. *Труды МИАН*, **313**, 124 (2021).
39. Кронберг Д.А., Курочкин Ю.В. *Квантовая электроника*, **48** (9), 843 (2018) [*Quantum Electron*., **48** (9), 843 (2018)].
40. Chefles A. *Phys. Lett. A*, **239** (6), 339 (1998).
41. Feng Y., Duan R., Ying M. *Phys. Rev. A*, **70** (1), 012308 (2004).
42. Herzog U., Bergou J.A. *Phys. Rev. A*, **71** (5), 050301 (2005).
43. Avanesov A.S., Kronberg D.A. *Lobachevskii J. Mathem*., **42** (10), 2285 (2021).
44. Балыгин К.А., Климов А.Н., Кулик С.П., Молотков С.Н. *Письма в ЖЭТФ*, **106** (2), 108 (2017) [*JETP Lett*., **106** (2), 120 (2017)].
45. Moroder T., Curty M., Lim C.C.W., Zbinden H., Gisin N. *Phys. Rev. Lett*., **109** (26), 260501 (2012).
46. Трушечкин А.С., Киктенко Е.О., Кронберг Д.А., Федоров А.К. *УФН*, **191** (1), 93 (2021) [*Usp. Phys*, **64** (1), 88 (2021)].